INFORMATION Management Conference

Continuous Monitoring Solutions for NNSA

Transformation through Partnerships

Lisa Ann Toland

April 18, 2012

U.S. DEPARTMENT OF ENERGY | Office of the Chief Information Officer

OVERVIEW

- Continuous Monitoring (CM) Defined
- NNSA CM Goals & Objectives
- CM and NNSA OCIO
- CM Project
  - Scope
  - Major Milestones and Schedule
  - Implementation Phases
  - Tool Requirements and Selection
  - Pilot Project Goals and Deliverables
  - Pilot Project Accomplishments

Continuous Monitoring Defined

- CM for the “Organization”
  - NNSA enhanced capability to measure risk in multiple areas
- CM for the “System”
  - Reduce the burden of Certification and Accreditation and Testing

Continuous Monitoring Defined (con't)

- NNSA'S CM Solution:
  - Gather essential security information
    - Cost-effective risk based operational decisions
  - Integrates with the NNSA Enterprise Architecture and System Life Cycle
    - Timely risk management and ongoing system authorization

NNSA CM Objectives

- Objectives include:
  - Monitoring of 100% networked system assets
  - Develop and integrate a solution by September 2013
  - Incorporate NNSA/DOE Policy
  - Reduce compliance-based reporting
  - Provide CyberScope and OMB reporting
  - Provide automated POA&M feeds to DOE
  - Provide an enterprise holistic view to make well informed business decisions

NNSA CM Goals

- Collaboration across the NNSA and Department of Energy (DOE)
- Monitors an environment that will result in:
  - Mission Focused Enterprise Architecture
  - Prioritized and manage IT investment
  - Implementing common solutions and fostering standards-based tools; and
  - More secure environment
    - system operations
    - data management
    - information sharing

CM Project Scope

- Develop, implement, field, test, and operate a continuous monitoring capability to:
  - Enhance NNSA cyber security posture based on a Risk Management Framework
  - Satisfy Congressional and OMB mandates
  - Satisfy GAO, OIG, DOE and NNSA FISMA compliance audits
  - Minimize Data Calls
    - Providing a robust continuous asset management capability
    - Timely correlation and reporting
    - Correlated comprehensive view of vulnerabilities and assets

Project Major Milestones

- Established a plan by June 1, 2011 in response to direction by OMB
- NNSA successfully implemented an automated CM pilot solution
- Implement all network unclassified systems
  - Started August 2011
  - Estimated completion by September 2012
- Implement all networked Classified systems
  - Start October 2012
  - Estimated completion by September 2013

CM Tool Selection Requirements

- Feed Information from a variety of sources (i.e. assessment objects)
- Use open specifications
- Offer Interoperability
- Support compliance
- Provide reporting
- Allows for data consolidation

CM Tool Selected

- RSA Archer eGRC
- Four Modules
  - Enterprise Management
  - Policy Management
  - Compliance Management
  - Threat Management
- Professional Services
- Basic and Advance Archer Training

Proposed CM Plan Supports Strategic Goals

- NNSA Strategic Goals Supported
  - Collapse and consolidate networks, applications, and services into virtualized environments
  - Encourage Enterprise Collaboration
  - Establish Risk Based Governance
  - Improve Business Processes

CM Project Deliverables

- Demonstration of the ability to publish information from the sites to the Enterprise
- Establish minimum Enterprise Data Feeds
- Identify Data Source for initial integration to archer
- Develop and demonstrate dashboards
- Create, implement and test connectors

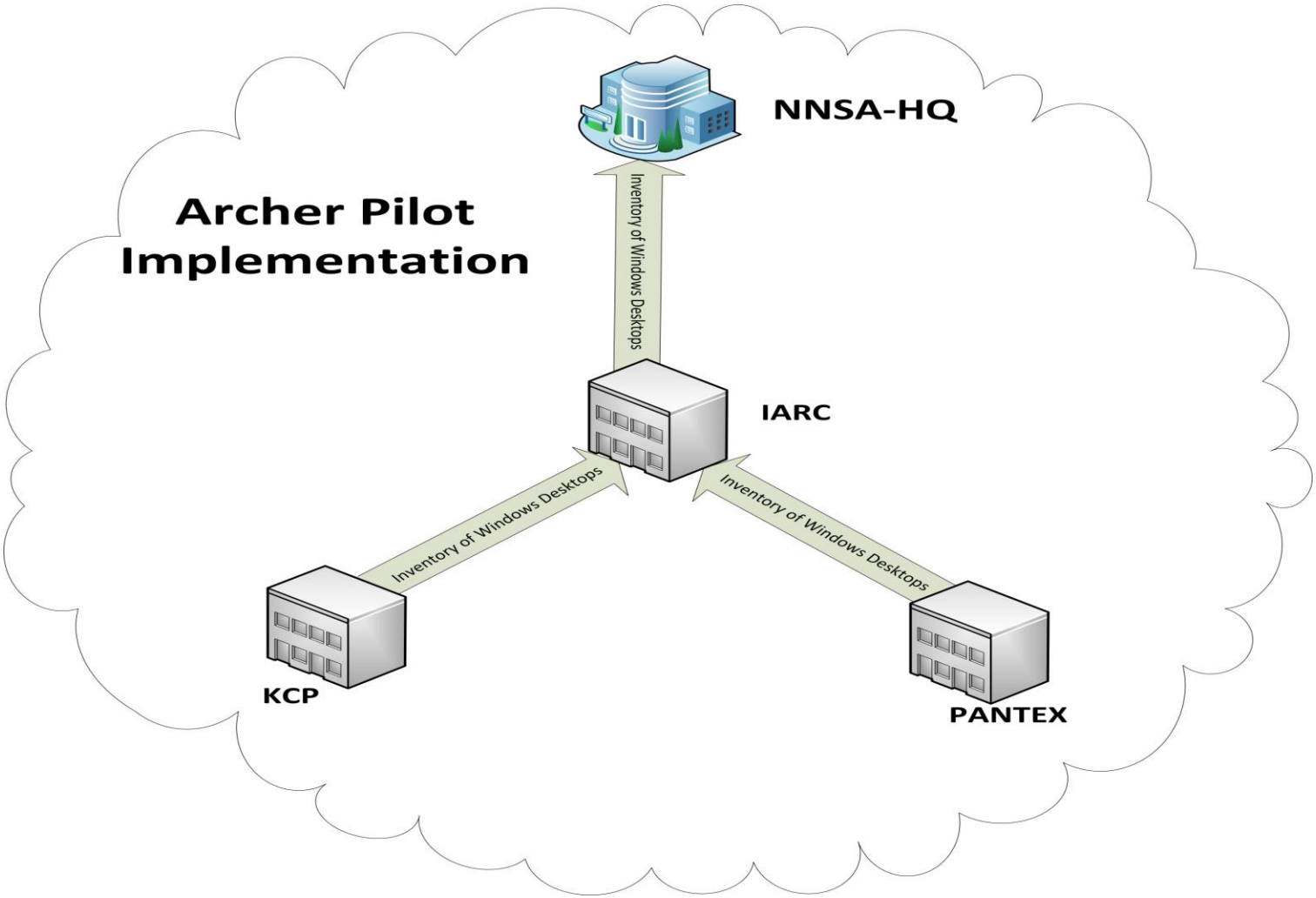
CM Deliverables Pilot Phase

- Implementation of Enterprise-wide deployment started with pilot sites:
  - Pantex
  - Kansas City Plant
  - IARC (Enterprise)

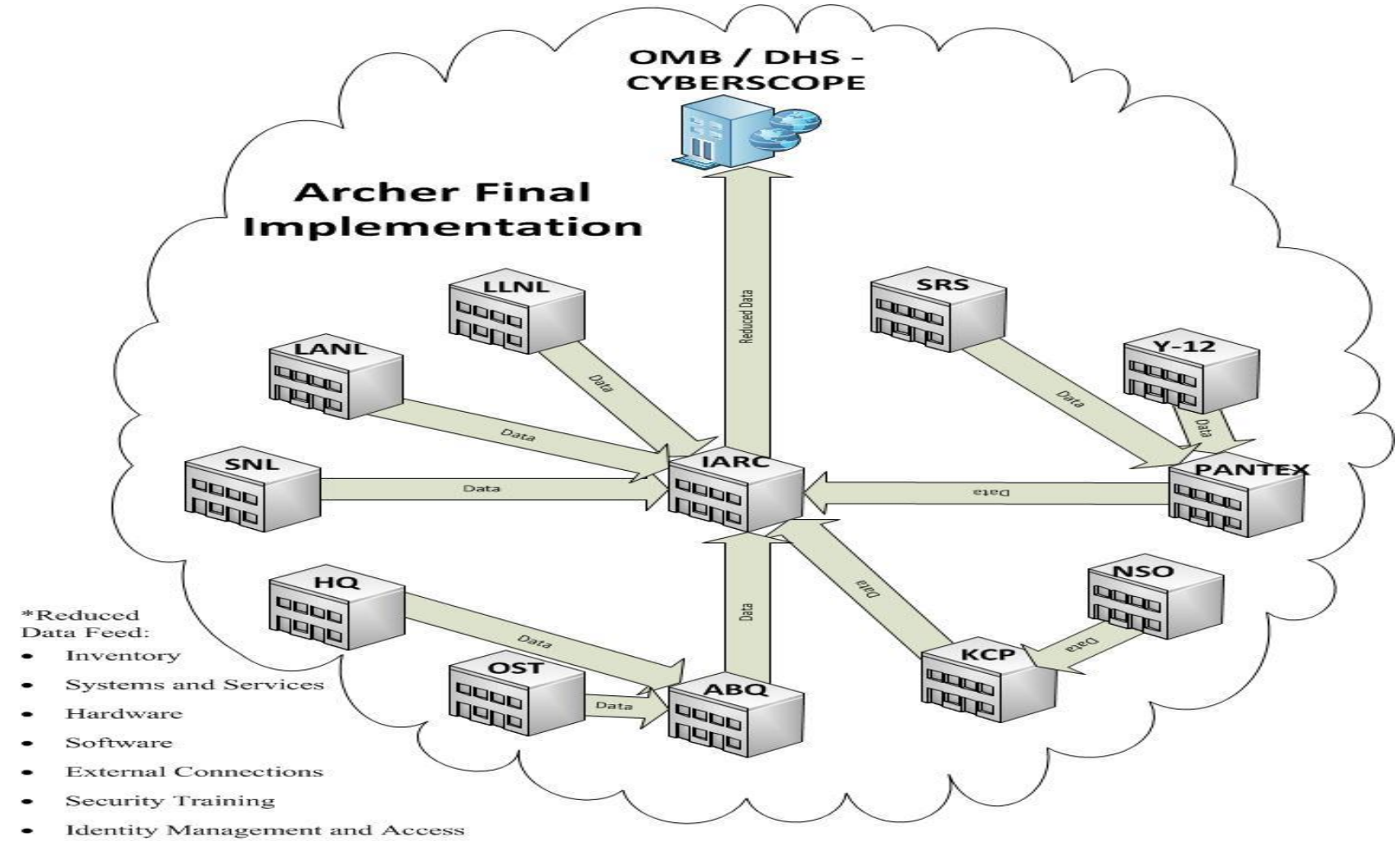
- Expansion Sites

NNSO	Savannah River
Headquarters	Y-12
Livermore	Sandia
LANL	Albuquerque

CM Pilot Implementation



CM Final Implementation



CM Project Accomplishments

- Created a Continuous Monitoring Working Group (CMWG) to Champion CM decisions for all Plants, Labs, and HQ entities
- Developed project matrix and stakeholder requirements up front prior to product selection
- Created a HQ driven collaboration across NNSA NSE Cyber community
- Decreased deployment strategies and stakeholder requirements up front during project pre-planning
- Kept entire Cyber, IT and CIO Management abreast of all activities during the project life cycle
- Use Kansas City wiki and collaborative share drive
- Completed Pilot in less than 30 days

Questions

Questions?

Questions

Continuous Monitoring Contacts

Federal Program Manager: John Doggett, jdoggett@pantex.doe.gov

Contractor Support: Lisa Toland lisa.toland@nnsa.doe.gov

Backup

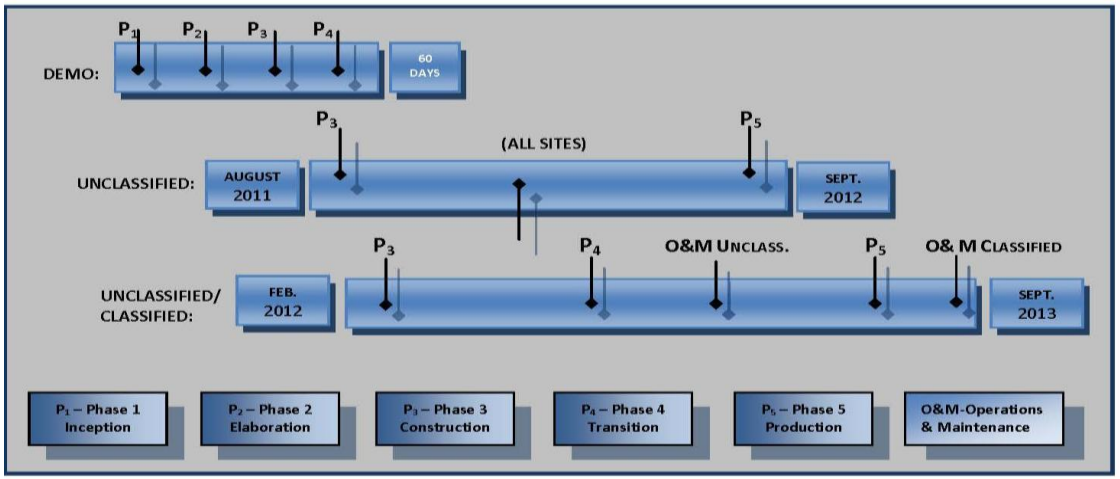
Project Purpose

Project Overview

- Reducing enterprise-wide cyber security risks is the primary objective of procuring an automated continuous monitoring solution. The automated solution will give NNSA the enhanced capability to measure risk in multiple areas with flexibility to address evolving risks; provide management metrics to make an informed decision to reduce risk; measure improvement; and provide risk scoring for field sites and the enterprise.
- Provide a common framework for reporting status

Project Management Plan

- Project Management Plan for Success
  - Critical Element
    - Inception
    - Elaboration
    - Construction
    - Transition
    - Production of the project as reported to Congress.



Business Case

- The Senate Energy and Water Appropriations bill of 2007, report 109-274
  - "develop vulnerability and risk management solution that continuously discovers and prioritizes network exposures including integrated network topology risk analysis"
    - Facilitate Certification and Accreditation under FISMA
      - Perform continuous monitoring requirement
        - NIST SP 800-37 Guidance

NNSA: OCIO Role for NNSA

- NNSA NSE depends on information and information systems to carry out mission and business functions
  - Information Systems are subject to serious threats the can effect:
    - Missions
    - Functions
    - Organizations assets
    - Individuals,
    - other organizations, and
    - the nations by
      - Compromising Confidelity, Integrity and Availability of information processed
      - stored or transmitted by those systems

NNSA: OCIO Role for NNSA

- NNSA is evolving from a compliance based to a risk based methodology that employs continuous monitoring to help guide decisions
- A component of the Risk Management approach to cyber security
  - Maintains an accurate picture of an organization's near real time security risk posture
    - Provides visibility into assets
    - Leverages use of automated data feeds to quantify risk
    - Ensures Effectiveness of security controls
    - Implements prioritized remedies

Project Milestones

- Pre-Planning
  - Pilot Strategy Meeting
  - Archer Basic Training
  - Pilot Stakeholder Meeting
  - Project Management Plan
  - Requirements Document
  - Draft Requirements Traceability Matrix
  - Design Document
  - Testing of Application functionality and security baseline

Project Milestones

Pilot

- Assemble Core/Site team and determine roles and responsibilities
- Implement Archer at sites
- Develop Change control process
- Deploy Tiger Teams to ensure project goals and costs are met
- Enterprise meeting (all sites)
- Establish minimum Enterprise data feeds (pilot only)
- Identify the data sources for initial integration into Archer
- Develop and demonstrate
  - Dashboards
  - Report and publish information
  - Workflow and notification capability